**AMENDMENTS TO THE CLAIMS:**

This listing of claims will replace all prior versions and listings of claims in the application:

27 - 30. (Canceled)

31. (Currently Amended) An expansion key generation apparatus, which generates expansion keys based on input keys, the apparatus comprising a plurality of cascade-connected key transform devices, each of the key transform devices comprising:

an exclusive-OR element for calculating an exclusive-OR of a constant determined for each of the key transform devices and a first key obtained from the input key;

a nonlinear transform unit for nonlinearly transforming an output from the exclusive-OR element using a predetermined substitution table;

an expansion unit for performing an expansion processing on an output from the nonlinear transform unit; and

an expansion key calculation unit for calculating the expansion key based on an output from the expansion unit and a second key obtained from the input key, wherein the expansion key calculation unit performs a shifting of a predetermined number of bits and

~~The expansion key generation apparatus according to claim 30, wherein the expansion unit~~ shifts the output from the nonlinear transform unit to the least significant bit by the number of bits that is half the number of bits of the output from the nonlinear transform unit, or by the number of bits obtained by adding an integer multiple of the number of bits of the output from the nonlinear transform unit to the half number of bits.

32. (Currently Amended) An expansion key generation apparatus, which generates expansion keys based on input keys, the apparatus comprising a plurality of cascade-connected key transform devices, each of the key transform devices comprising:

an exclusive-OR element for calculating an exclusive-OR of a constant determined for each of the key transform devices and a first key obtained from the input key;

a nonlinear transform unit for nonlinearly transforming an output from the exclusive-OR element using a predetermined substitution table;

an expansion unit for performing an expansion processing on an output from the nonlinear transform unit; and

an expansion key calculation unit for calculating the expansion key based on an output from the expansion unit and a second key obtained from the input key,

~~The expansion key generation apparatus according to claim 27,~~ wherein the expansion key calculation unit adds with carry-up the output from the expansion unit and the second key.

33 - 39. (Canceled)

40. (Currently Amended) An expansion key generation program, which causes a computer to generate expansion keys based on input keys using a plurality of cascade-connected key transform devices, the program comprising:

program code for calculating an exclusive-OR of a constant determined for each of the key transform devices and a first key obtained from the input key;

program code for nonlinearly transforming a result of an exclusive-OR using a predetermined substitution table;

program code for performing an expansion processing on a result of a nonlinear transform, wherein the program code for performing the expansion processing comprises program code for shifting a result of a nonlinear transform by a predetermined number of bits

~~The program according to claim 39, wherein the program code for performing an expansion processing comprises program code for shifting a result of a nonlinear transform by the number of bits~~ that is half the number of bits of a result of a nonlinear transform, or by the number of bits obtained by adding an integer multiple of the number of bits of the result of the nonlinear transform to the half number of bits[[.]];

program code for calculating the expansion key based on a result of expansion processing and a second key obtained from the input key; and

program code for shifting the input key to a least significant bit or a most significant bit and inputting the shifted key to the key transform device of a next stage.

41. (Currently Amended) An expansion key generation program, which causes a computer to generate expansion keys based on input keys using a plurality of cascade-connected key transform devices, the program comprising:

program code for calculating an exclusive-OR of a constant determined for each of the key transform devices and a first key obtained from the input key;

program code for nonlinearly transforming a result of an exclusive-OR using a predetermined substitution table;

program code for performing an expansion processing on a result of a nonlinear transform; and

program code for calculating the expansion key based on a result of expansion processing and a second key obtained from the input key,

~~The program according to claim 36,~~ wherein the program code for calculating the expansion key comprises program code for adding with carry-up a result of an expansion and the second key.

42 - 46. (Canceled)